Meldung größerer Vorfälle im Zahlungssystem girocard der Deutschen Kreditwirtschaft

(gekürzte und übersetzte Fassung der englischen Fassung des EZB-Rahmenwerks)

Stand 9. November 2020

Einleitung

Das „Major incident reporting framework for payment schemes and retail payment systems" ("Regelwerk") des Eurosystems stellt seit 1. Januar 2019 den Rahmen für die Meldung wichtiger Vorfälle durch die Betreiber von Zahlungssystemen dar. Dieser ist Teil der umfassenden Anforderungen an die Überwachung des Eurosystems für Zahlungsverkehrssysteme. Ziel ist, die Stabilität des Zahlungsverkehrs in Europa zu gewährleisten. Das Regelwerk baut auf den Anforderungen des „Eurosystem oversight policy framework" aus dem Jahr 2016 auf und berücksichtigt weitestgehend den Melderahmen, der mit den Anforderungen aus der PSD2 einhergeht.

Seit dem 1. Januar 2019 sind die Betreiber von Zahlungssystemen und Massenzahlungssystemen verpflichtet, größere Sicherheitsvorfälle im Zahlungsverkehr gemäß den Anforderungen und Definitionen des überarbeiteten Regelwerks zu klassifizieren und ihrem jeweiligen federführenden Aufsichtsorgan zu melden.

Das Regelwerk ergänzt die bestehenden Berichtsanforderungen, die in den bestehenden Überwachungsstandards, Rahmenwerken und Bewertungsleitfäden des Eurosystems enthalten sind.

Betrifft ein Vorfall die Funktionsweise des Systems und/oder des Massenzahlungssystems, so muss der Vorfall sowohl der federführenden Aufsichtsbehörde als auch der zuständigen nationalen Behörde[1] gemeldet werden, sofern die jeweiligen Schwellenwerte für die Meldung größerer Vorfälle erreicht werden.

Adressaten des Regelwerkes sind die Betreiber, d.h. sog. Governance Authorities (nachfolgend als „GA" bezeichnet) von Zahlungssystemen oder -verfahren.

Die GA und damit der Betreiber für das girocard-System sowie für das Deutsche Geldautomatensystem ist die Deutsche Kreditwirtschaft (DK). Das Regelwerk gilt für die DK in ihrer Rolle als Systembetreiber und insofern auch für die Teilnehmer am System (kartenausgebende Institute, Händlerbanken, Netzbetreiber, Kopf- und Übergabestellen usw.). Die für das girocard-System / Geldautomatensystem relevanten Klassifizierungsanforderungen finden sich unmittelbar in Kapitel 3.2. Da die Verarbeitung von Transaktionen (Clearing, Settlement) über die bestehenden Massenzahlungsverkehrssysteme abgewickelt werden, gelten auch die für diese Systeme geltenden Klassifizierungsanforderungen gemäß Kapitel 3.1.

Das Aufsichtsorgan für das girocard-System ist die Deutsche Bundesbank.

1. Geltungsbereich

Das Regelwerk bezieht sich auf größere Betriebs- und Sicherheitszwischenfälle, einschließlich Cyber-Zwischenfälle, deren negative Auswirkungen bereits eingetreten sind oder wahrscheinlich eintreten werden. Diese Zwischenfälle fallen zudem in den Anwendungsbereich der PSD2 und der „EBA-Leitlinien für die Meldung schwerwiegender Vorfälle gemäß Richtlinie EU 2015/2366 (PSD2)" vom 19. Dezember 2017 (deutsche Version).

Frühwarnungen[2] sind von der Berichterstattung nach dem Regelwerk ausgeschlossen, da der Schwerpunkt auf tatsächlichen Vorfällen liegt.

[1] Benannt unter PSD2 – in Deutschland: BaFin

[2] Wie im derzeitigen Rahmen vorgesehen - z.B. gefundene Schwachstellen, Verwundbarkeiten und Missbräuche, die noch keine Betriebsunterbrechung oder -verlust gebracht haben.

Das Regelwerk ist an die Betreiber von. Zahlungssystemen und Massenzahlungssystemen adressiert, die der Überwachung durch die EZB bzw. der nationalen Notenbanken unterliegen.

2. Definitionen

Die o.g. „Leitlinien für die Meldung schwerwiegender Vorfälle gemäß der Richtlinie EU/2015/2366 (PSD2)" definieren den Begriff "Betriebs- oder Sicherheitsvorfall", der weitgehend auf der Definition des Begriffs "größerer Sicherheitsvorfall im Zahlungsverkehr" beruht:

"Ein singuläres Ereignis oder eine Reihe von miteinander verbundenen Ereignissen, das/die von der Governance Authority / den Betreibern[3] des Massenzahlungssystems nicht geplant ist und das/die sich nachteilig auf die Integrität, Verfügbarkeit, Vertraulichkeit, Authentizität und/oder Kontinuität der zahlungsbezogenen Dienste auswirkt oder wahrscheinlich auswirken wird".

In Bezug auf Zahlungssysteme sollten zahlungsbezogene Dienstleistungen als all jene Dienstleistungen

- des Zahlungssystembetreibers verstanden werden, die zur Abwicklung eines Geldtransfers zwischen den Teilnehmern erforderlich sind. Zu diesen Dienstleistungen gehören unter anderem solche, die die Übermittlung des Zahlungsauftrags ermöglichen, sowie solche, die das Clearing, Netting und Settlement ermöglichen. Andere Dienste, die als akzessorisch betrachtet werden können (z.B. Fakturierung, statistische Berichterstattung), gelten als nicht in den Anwendungsbereich fallend.
- verstanden werden, die erforderlich sind, um die korrekte Ausführung der vom System abgedeckten Zahlungsdienstleistung zu gewährleisten. Zu diesen Dienstleistungen gehören unter anderem die Herausgabe eines Zahlungsinstruments und die Ausstellung der damit verbundenen personalisierten Sicherheitszertifikate, die Zertifizierung und der Betrieb von Terminals, die Autorisierung, Authentifizierung sowie das Clearing und die Abwicklung der Zahlungstransaktion. Andere Dienstleistungen, die als akzessorisch betrachtet werden können (z.B. Fakturierung, statistische Berichterstattung), gelten als nicht in den Anwendungsbereich fallend.

3. Klassifizierungskriterien

Betreiber von Massenzahlungssystemen/Zahlungssystemen müssen die Art eines Betriebs- oder Sicherheitsvorfalls feststellen und seine Wesentlichkeit anhand der folgenden Kriterien bewerten:

- Anzahl der betroffenen Transaktionen,
- Anzahl der betroffenen Teilnehmer,
- Ausfallzeit des Dienstes,
- verzögerte Abschaltung,
- hohes Maß an interner Eskalation,
- andere relevante Finanzmarktinfrastrukturen/Zahlungssysteme, die möglicherweise betroffen sind, und Auswirkungen auf den Ruf[4].

Die Governance Authority muss die Wesentlichkeit des festgestellten Vorfalls anhand der Klassifizierungskriterien bewerten und darüber gegenüber ihrem Aufsichtsorgan Bericht erstatten.

3.1 Massenzahlungssysteme

a) Betroffene Transaktionen

Anzahl der betroffenen Transaktionen als Prozentsatz des regulären Niveaus der verarbeiteten Transaktionen. Unter "betroffenen Transaktionen" sind diejenigen Transaktionen zu verstehen, die direkt oder indirekt von dem Vorfall betroffen sind oder wahrscheinlich betroffen sein werden. Insbesondere Transaktionen, die nicht initiiert oder verarbeitet werden konnten, bei denen der Inhalt der Zahlungsnachricht geändert wurde, die in betrügerischer Weise angeordnet wurden (unabhängig

[3] Gemäß der Definition im "Harmonised oversight approach and oversight standards for payment instruments"

[4] Dieser Satz von qualitativen und quantitativen Kriterien wurde auf der Grundlage der gegenwärtigen Praktiken der Aufseher und Aufsichtsbehörden und unter Berücksichtigung der Zwischenlösung gewählt.

davon, ob die Gelder wieder eingezogen wurden oder nicht) oder bei denen die ordnungsgemäße Ausführung durch den Vorfall verhindert oder in anderer Weise behindert wird. Im Hinblick auf die Unfähigkeit, Transaktionen einzuleiten und/oder zu verarbeiten, sollte die Meldung auch Informationen über den Zeitrahmen enthalten (d.h. wie sehr sich die Verarbeitung der betroffenen Transaktionen verzögert hat).

Der regelmäßige Umfang der verarbeiteten Transaktionen sollte als täglicher Durchschnitt aller vom Massenzahlungssystem innerhalb eines Jahres verarbeiteten Transaktionen verstanden werden.

b) Betroffene Teilnehmer

Anzahl der betroffenen Teilnehmer in Prozent der Gesamtzahl der Teilnehmer. Unter "betroffenen Teilnehmern" sollten diejenigen verstanden werden, die die Folgen des Vorfalls erlitten haben oder wahrscheinlich noch erleiden werden.

Im Hinblick auf die Unfähigkeit, Transaktionen einzuleiten und/oder zu verarbeiten, sollte die Berichterstattung auch Informationen über den Zeitrahmen enthalten (d.h. wie lange die Teilnehmer betroffen sind).

Die Methodik zur Beurteilung dieses Kriteriums sieht zwei Unterschwellen für die Klassifizierung von Vorfällen mit "höherer Auswirkung" vor, um sowohl die inländischen als auch die grenzüberschreitenden Auswirkungen der Vorfälle zu messen.

c) Ausfallzeit des Dienstes

Zeitraum, in dem das System für die Teilnehmer nicht verfügbar ist oder gewesen sein kann oder in dem der Betreiber in der Lage ist oder nicht in der Lage war, Transaktionen zu verarbeiten. Die Service-Ausfallzeit sollte ab dem Zeitpunkt des Beginns der Ausfallzeit gezählt werden, und wenn es nicht möglich war, den Zeitpunkt des Beginns der Service-Ausfallzeit zu bestimmen, könnte die Service-Ausfallzeit ausnahmsweise ab dem Zeitpunkt der Feststellung der Ausfallzeit gezählt werden.

d) Verzögerter Abschluss

Vorfall, der eine gewisse Verzögerung bei der Annahmeschlusszeit für den Vergleich am selben Tag verursacht.

e) Hohes internes Eskalationsniveau

Ob der Vorfall den leitenden Angestellten des Systembetreibers außerhalb eines periodischen Meldeverfahrens und kontinuierlich während der gesamten Dauer des Vorfalls gemeldet wurde oder wahrscheinlich gemeldet wird. Es wird davon ausgegangen, dass dies unter anderem in einer Situation geschieht, in der ein kritischer Prozess betroffen ist, ein erneutes Auftreten derselben Art von Vorfall vorliegt oder die Störung während eines besonders kritischen Zeitfensters (z.B. in der Nähe einer Ausschaltzeit) eintritt. Darüber hinaus sollte geprüft werden, ob durch die Auswirkungen des Vorfalls auf zahlungsbezogene Dienstleistungen ein Krisenmodus ausgelöst wurde oder wahrscheinlich ausgelöst wird.

Sollte die Annahmeschlusszeit für die taggleiche Abwicklung verzögert sein, wird ein solcher Vorfall aufgrund seiner Bedeutung in der Regel intern eskaliert.

f) Andere relevante Finanzmarktinfrastrukturen/Zahlungssysteme, die potenziell betroffen sind.

Der Betreiber sollte unter anderem beurteilen, ob sich der Vorfall wiederholt hat oder wahrscheinlich wiederholen wird, ob er das reibungslose Funktionieren anderer Finanzmarktinfrastrukturen und/oder Zahlungssysteme beeinträchtigt hat oder wahrscheinlich beeinträchtigen wird oder ob er die Solidität des Finanzsystems insgesamt beeinträchtigt hat oder wahrscheinlich beeinträchtigen wird.

Die bestehenden Interdependenzen sollten berücksichtigt werden (z.B. ob die betroffene Komponente/Software proprietär oder allgemein verfügbar ist, ob das kompromittierte Netzwerk intern oder extern ist, oder ob der Vorfall die Fähigkeit der Teilnehmer, ihren Verpflichtungen in anderen Infrastrukturen/Zahlungssystemen, bei denen sie Mitglied sind, nachzukommen, beeinträchtigt hat oder wahrscheinlich beeinträchtigen wird).

g) Auswirkungen auf die Reputation

Insbesondere sollte die Wahrscheinlichkeit, dass der Vorfall dem Markt Schaden zufügt und letztlich das Vertrauen in das Zahlungssystem untergräbt, als ein guter Indikator für das Potenzial betrachtet werden, den Ruf des Systems zu beeinflussen.

3.2 Zahlungssysteme

a) Betroffene Transaktionen

Anzahl der betroffenen Zahlungen, Terminals[5], Geräte der Dienstleistungsnutzer[6] und - im Falle von Kartenzahlungssystemen - Zahlungskarten als prozentualer Anteil am regelmäßigen Umfang der gemäß den Regeln des Systems durchgeführten Zahlungstransaktionen / Gesamtzahl der Terminals / Geräte der Dienstleistungsnutzer / Karten[7]. Der Begriff "Transaktionen" sollte gemäß den in den Regeln des Systems festgelegten Definitionen verstanden werden. Als "betroffene Transaktionen" sollten Transaktionen verstanden werden, die direkt oder indirekt von dem Vorfall betroffen sind oder wahrscheinlich betroffen sein werden und die insbesondere nicht veranlasst oder verarbeitet werden konnten, bei denen der Inhalt der Zahlungsnachricht geändert wurde, die in betrügerischer Weise angeordnet wurden denen die ordnungsgemäße Ausführung durch den Vorfall verhindert oder in anderer Weise behindert wird. Im Hinblick auf die Unfähigkeit, Transaktionen einzuleiten und/oder zu verarbeiten, sollte die Meldung auch Informationen über den Zeitrahmen enthalten (d.h. wie sehr sich die Verarbeitung der betroffenen Transaktionen verzögert hat).

b) Betroffene Teilnehmer[8]

Anzahl der betroffenen Teilnehmer in Prozent der Gesamtzahl der jeweiligen Teilnehmer. Unter "betroffenen Teilnehmern" sollten diejenigen verstanden werden, die unter den Folgen des Vorfalls gelitten haben oder wahrscheinlich leiden werden. Es sollten alle Teilnehmer des Systems berücksichtigt werden, unabhängig von der Art oder dem Status der zugrundeliegenden Lizenz und/oder der Rolle, die sie für das Funktionieren des Systems spielen (z.B. Emittenten, Erwerber, Liquiditätsgeber, Verrechnungsbanken usw.).

c) Ausfallzeit des Dienstes

Zeitraum, in dem die mit dem System verbundenen Dienstleistungen für die Teilnehmer und/oder Endnutzer möglicherweise nicht verfügbar sind oder in dem der Zahlungsvorgang von den Systemteilnehmern nicht ausgeführt werden kann.

…

f) Andere relevante Finanzmarktinfrastrukturen/Zahlungssysteme, die potenziell betroffen sind

Die systemischen Implikationen, die der Vorfall haben kann, d.h. sein Potenzial, entweder direkt oder indirekt über das ursprünglich betroffene System hinaus zu wirken. Die Governance Authority[9] sollte unter anderem beurteilen, ob sich der Vorfall wiederholt hat oder wahrscheinlich wiederholen wird, ob er das reibungslose Funktionieren anderer Finanzmarktinfrastrukturen und/oder Zahlungssysteme beeinträchtigt hat oder wahrscheinlich beeinträchtigen wird.

Die bestehenden Interdependenzen sollten nach bestem Wissen der GA berücksichtigt werden (z.B. ob die betroffene Komponente/Software proprietär oder allgemein verfügbar ist, ob das kompromittierte Netzwerk intern oder extern ist, oder ob der Vorfall die Fähigkeit der Teilnehmer, ihren Verpflichtungen in anderen relevanten Infrastrukturen/Zahlungssystemen nachzukommen, beeinträchtigt hat oder wahrscheinlich beeinträchtigen wird).

g) Auswirkungen auf die Reputation

Grad der Sichtbarkeit, den der Vorfall nach bestem Wissen und Gewissen bei den Teilnehmern und anderen relevanten Interessengruppen erreicht hat oder wahrscheinlich erreichen wird. Insbesondere sollte die Wahrscheinlichkeit, dass der Vorfall dem Markt Schaden zufügt und letztlich das Vertrauen in das Zahlungssystem untergräbt, als ein guter Indikator für das Potenzial betrachtet werden, den Ruf des Systems zu beeinflussen.

5 Geldautomaten, physische POS-Terminals und virtuelle POS-Terminals

6 Im Sinne der Definition für "Zahlungsinstrument" in der PSD2, Art. 4 (14)

7 Einschließlich physischer und virtueller Karten

8 Die am Zahlungssystem teilnehmenden Zahlungsdienstleister

9 Adressiert ist hiermit die Deutsche Kreditwirtschaft

Die Governance Authority sollte berücksichtigen, ob:

i) der Vorfall einen sichtbaren Prozess beeinträchtigt hat und daher wahrscheinlich Medienberichterstattung erhalten oder bereits erhalten hat (wobei nicht nur traditionelle Medien wie Zeitungen, sondern auch Blogs, soziale Netzwerke usw. berücksichtigt werden),

ii) regulatorische und/oder vertragliche Verpflichtungen entweder von den Teilnehmern oder von den Endnutzern versäumt wurden oder wahrscheinlich versäumt werden,

iii) Sanktionen gegen die Teilnehmer verhängt wurden oder wahrscheinlich verhängt werden, oder

iv) d ie gleiche Art von Vorfall bereits früher aufgetreten ist.

3.3 Beurteilung der Erheblichkeit eines Vorfalls

Betreiber / Governance Authorities müssen die Wesentlichkeit eines Vorfalls feststellen. Sie müssen für jedes einzelne Kriterium bestimmen, ob die in der Tabelle aufgeführten relevanten Schwellenwerte erreicht sind oder wahrscheinlich erreicht werden, bevor der Vorfall gelöst ist. Diese Schwellenwerte sind zudem nach zwei möglichen Schweregraden gegliedert, von denen der eine niedriger ("Niedrigere Auswirkungsstufe") als der andere ("Höhere Auswirkungsstufe") ist. Sollten die tatsächlichen Daten nicht verfügbar sein, können die Betreiber/Governance Authorities (GA) auf Schätzungen zurückgreifen. Diese sollten darauf abzielen, die Niveaus vorherzusagen, die die verschiedenen Kriterien erreichen können, bevor der Vorfall gelöst ist.

Der Betreiber / GA würde diejenigen Vorfälle als schwerwiegend einstufen, die entweder i) ein oder mehrere Kriterien auf der Ebene "Höhere Auswirkung" oder ii) drei oder mehr Kriterien auf der Ebene "Niedrigere Auswirkung" erfüllen (bei Stapelverarbeitungssystemen - zwei oder mehr Kriterien "Niedrigere Auswirkung"). Im Zweifelsfall sollte die berichtende Stelle auf der Grundlage der verfügbaren vorläufigen Informationen oder Schätzungen berichten und sich für die höhere Klassifizierung entscheiden.

3.4 Schwellenwerte gemäß Regelwerk

Für die Meldung an die Deutsche Kreditwirtschat ist das „Formular zur Störungsmeldung" zu verwenden.

Es gelten folgende Schwellenwerte:

	Massenzahlungssystem		**Kartenzahlungssystem**	
	Niedrige Auswirkung	**Hohe Auswirkung**	**Niedrige Auswirkung**	**Hohe Auswirkung**
Transaktionen[10] / Endgeräte / Geräte der Dienstleistungsnutzer / Karten (Bei betrieblichen Vorfällen ist dieses Kriterium nur anwendbar, wenn die Verarbeitung[11] der betroffenen Transaktionen während des laufenden Geschäftstages	≥ 5 % der betroffenen RPS-Transaktionen in einer einzigen Gerichtsbarkeit [13]	≥ 10 % der betroffenen RPS-Transaktionen in einer einzigen Gerichtsbarkeit; oder ≥ 2% der Transaktionen in	≥ 5 % der betroffenen Transaktionen / Terminals / Geräte der Dienstleistungsnutzer / Karten des Zahlungssyste	≥ 10 % der betroffenen Transaktionen / Terminals / Geräte der Dienstleistungsnutzer / Karten des Zahlungssyste

10 Dieses Kriterium gilt nicht für Stapelverarbeitungssysteme

11 Bei Zahlungssystemen schließt dies auch Situationen ein, in denen die Einleitung von Transaktionen nicht möglich ist.

13 Transaktionen, die durchgeführt werden, wenn beide Teilnehmer (PSP des Zahlers und PSP des Zahlungsempfängers) einer individuellen Gerichtsbarkeit angehören (z.B. in einem einzigen Land ansässig sind)

	Massenzahlungssystem		**Kartenzahlungssystem**	
	Niedrige Auswirkung	**Hohe Auswirkung**	**Niedrige Auswirkung**	**Hohe Auswirkung**
unmöglich oder um mehr als 2 Stunden verzögert ist)[12]		der gesamten EU betroffen	ms in einer einzigen Gerichtsbarkeit	ms in einer einzigen Gerichtsbarkeit; oder ≥ 2% der Transaktionen / Terminals / Karten in der gesamten EU betroffen
Teilnehmer[14] (Bei betrieblichen Vorfällen ist dieses Kriterium nur dann anwendbar, wenn die Verarbeitung[11]**Fehler! Textmarke nicht definiert.** der betroffenen Transaktionen während des laufenden Geschäftstages unmöglich oder um mehr als 2 Stunden verzögert ist) [12]	≥ 5 % der betroffenen Teilnehmer in einer einzigen Gerichtsbarkeit [13]	≥ 10 % der Teilnehmer sind in einer einzigen Gerichtsbarkeit [15] betroffen; oder ≥ 2% der Teilnehmer in der gesamten EU betroffen	≥ 5 % der Teilnehmer in einer einzigen Gerichtsbarkeit betroffen	≥ 10 % der Teilnehmer sind in einer einzigen Gerichtsbarkeit betroffen; oder ≥ 2% der Teilnehmer in der gesamten EU betroffen
Ausfallzeiten [16]	Nicht zutreffend	> 2 Stunden für RPS, die im Rahmen von Sofortzahlungssystemen arbeiten: > 1 Stunde	Nicht zutreffend	> 2 Stunden für Instant Payment: > 1 Stunde
Verzögerte Abschaltung [16]	Nicht zutreffend	Die Ausschaltzeit ist um mindestens	Nicht zutreffend	Die Ausschaltzeit ist um

12 Bezieht sich auf beide Unterschwellen - sowohl für Transaktionen unter einer einzigen Gerichtsbarkeit als auch für Transaktionen innerhalb der EU.

14 Dieses Kriterium gilt nicht in Fällen, in denen der Zahlungsverkehrsdienstleister auch das System betreibt und der einzige Teilnehmer an einem solchen System ist (z. B. Drei-Parteien-Systeme).

15 Dieser Unterschwellenwert gilt nicht für Stapelverarbeitungssysteme.

16 Dieses Kriterium gilt nicht für Zahlungssysteme ohne operative Funktionen

	Massenzahlungssystem		**Kartenzahlungssystem**	
	Niedrige Auswirkung	**Hohe Auswirkung**	**Niedrige Auswirkung**	**Hohe Auswirkung**
		1 Stunde verzögert.		mindestens 1 Stunde verzögert.
Hohe interne Eskalationsstufe	Ja	Ja, und es ist wahrscheinlich, dass ein Krisenmodus (oder ein gleichwertiger Modus) in Anspruch genommen wird.	Ja	Ja, und es ist wahrscheinlich, dass ein Krisenmodus (oder ein gleichwertiger Modus) in Anspruch genommen wird.
Andere relevante Finanzmarktinfrastrukturen/Zahlungssysteme, die potenziell betroffen sind	Ja	Nicht zutreffend	Ja	Nicht zutreffend
Auswirkungen auf die Reputation	Ja	Nicht zutreffend	Ja	Nicht zutreffend